# Department of Homeland Security Daily Open Source Infrastructure Report for 28 March 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

**Daily Highlights**

- The Rocky Mountain News reports federal agents are in a nationwide manhunt for a serial bomber −− the suspect in five bombs in Grand Junction, Colorado, and another in Tennessee, who is considered “extremely dangerous” and a potential threat to airports. (See item 21)
- USA TODAY reports federal aviation investigators say that a plan by jet manufacturer Airbus that urges airlines to inspect certain jets for a possible serious safety problem is "inadequate" and that the inspections need to be done faster. (See item 22)
- The Los Angeles Times reports the spread of avian influenza to at least 29 new countries in the last seven weeks is prompting a reassessment of the strategy that has guided efforts to contain the disease, toward instead managing a disease that will probably be everywhere. (See item 34)



## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 28, Oakland Tribune (CA)* — **Fire shuts down two BART stations in East Bay, California.** A power substation caught fire near the South Hayward, CA BART station Friday, March 24, causing the station and two others to be closed for a little more than an hour.

Stranded noontime passengers took shuttle buses to and from the downtown Hayward, South Hayward, Union City, and Fremont stations as firefighters put out the electrical blaze. The substation is one of more than 40 across the Bay Area that BART uses to power trains via the track's third rail. The fire was reported at 12:04 p.m. PST and was fully extinguished before 1:30 PST. The agency halted all trains headed south of downtown Hayward and called for a "bus bridge" at 12:14 p.m. Investigators are trying to determine what caused the blaze. The last disruptive electrical fire on a BART line was in San Leandro in October, when a piece of equipment fell off a train and damaged the third rail. On Thursday, March 9, a debris fire in a BART tunnel below downtown San Francisco caused evacuations and transit delays on both sides of the Bay.
Source: http://www.zwire.com/site/news.cfm?newsid=16374884&BRD=1686&PAG=740&dept_id=226967&

2. *March 27, Associated Press* — **France takes lead in nuclear future.** Twenty years after the Chernobyl nuclear plant disaster, a new crop of leaders in North America, Europe and Asia is thinking nuclear. France has done perhaps the most to push back the pendulum. As the only European country that continued making nuclear plants after Chernobyl, France has up−to−date expertise that it is eager to export, and the market is ballooning. With energy worries topping the world's agenda, some are reconsidering nuclear power, persuaded by improved safety and the fear that fossil fuels pose greater dangers to the planet. France's key partner in promoting the renaissance is unexpected: the United States. After two decades on the defensive, French and U.S. industries are cooperating closely in hopes of a new boom in nuclear power. France is selling more than electricity and reactor parts. It is preaching an updated version of the long−abandoned nuclear idea. Energy analyst David Bryant said the French government has made safety paramount because it is the key to keeping the crucial industry afloat. The industry says Generation IV will be the most efficient, will produce less waste and will be simplified to better handle and prevent accidents.
Source: http://www.washtimes.com/functions/print.php?StoryID=2006032 7−120713−4147r

3. *March 26, USA TODAY* — **Official warns of unsecured nuclear reactors.** One−third of the world's 130 civilian nuclear research reactors lack security upgrades needed to prevent theft of materials that terrorists could use to build an atomic bomb, the chief U.S. nuclear proliferation official says. Linton Brooks spoke Friday, March 3 about reducing the nuclear weapons stockpile in Oak Ridge, TN. In an interview with USA TODAY, Linton Brooks, director of the National Nuclear Security Administration, said most of these reactors use highly enriched uranium, the easiest fuel used to make atomic bombs. All reactors in the U.S., Russia, and Eastern Europe have adequate security, according to the National Nuclear Security Administration and Holly Harrington of the Nuclear Regulatory Commission. That's an improvement over 10 years ago when many Soviet bloc research reactors were particularly vulnerable to theft. Eight reactors not in those countries are slated to receive improved perimeter fencing, surveillance cameras, and material storage. That leaves 47 reactors with inadequate or questionable security in China, Ghana, Jamaica, Pakistan and Uzbekistan, according to an International Atomic Energy Agency (IAEA) list. There are also research reactors in countries hostile toward the United States, including Iran and North Korea. The IAEA says 38 countries have reactors that use highly enriched uranium.
Source: http://www.usatoday.com/news/washington/2006−03−26−nuclear−s ecurity_x.htm

4. *March 24, Contra Costa Times (CA)* — **Cities explore energy options.** Five years ago cities in California were worrying about how to keep the lights on and energy prices down for their residents. In the East Bay and elsewhere, city leaders considered building their own, or becoming partners in, small local power plants. The rolling blackouts of summer 2001 are a thing of the past, but cities are still considering measures to help make sure those dark days are not revisited. Pleasanton, for example, is researching the merits of becoming a "community choice aggregator." The city would still need to use PG&E lines, but it would have more control over local energy. A similar plan was presented in January to the Livermore City Council. Other cities, such as Oakland, Berkeley, and Emeryville already have participated in, and accepted, a feasibility study sponsored by the Local Government Commission in Sacramento examining becoming an aggregate. "I think there has been a movement away from the attitude of, 'Hey, let's just keep the lights on,' to 'Let's find a sustainable, more stable energy system,'" said Scott Baker, assistant director for public works in Pleasanton.
Source: http://powermarketers.netcontentinc.net/newsreader.asp?ppa=8knpp%5E%5BgklhmmlVUjf%216%3C%22bfel%5Dv

5. *March 24, Charlotte Observer (NC)* — **Duke Energy merger gets final approval.** Duke Energy Corp. got the final regulatory approval needed Friday, March 24, to complete its merger with Cinergy Corp. of Ohio. The merger will create one of the country's biggest electricity companies, with regulated power utilities running from Indiana to the S.C./Georgia border. The North Carolina Utilities Commission was the last regulatory body to rule on the merger, capping a series of OKs from state and federal bodies. The commission said it will start an investigation next year to determine whether Duke Power's rates are reasonable.
Source: http://powermarketers.netcontentinc.net/newsreader.asp?ppa=8knpp%5E%5BgklltyuVUjf%216%3C%22bfel%5Dv

[Return to top]

## Chemical Industry and Hazardous Materials Sector

6. *March 26, CBS 5 (CA)* — **Sulfur dioxide leak in California prompts shelter−in−place warning.** The Shell oil refinery in Martinez, CA, sounded an emergency siren Sunday, March 26, warning nearby residents to shelter−in−place because of a sulfur dioxide leak at the refinery. The alert was lifted shortly after 5 p.m. PST.
Source: http://cbs5.com/topstories/local_story_085203431.html

7. *March 25, Altoona Mirror (AL)* — **Plant worker dies after exposure to chemical on the job.** Lee Henninger died Friday evening, March 24, at his Tyrone, AL, home after he was exposed to thiophosphoryl chloride, a fertilizer additive, earlier that day at the Tyrone Albemarle Corp. chemical plant.
Source: http://www.altoonamirror.com/articles.asp?ID=15571

8. *March 25, Toledo Blade (OH)* — **Gasoline spillage estimate doubled.** A 50−year−old BP Inc. pipeline in West Toledo, OH, that split apart Thursday, March 23, has leaked almost twice as much gasoline as originally thought. BP Friday, March 24, raised the estimated total for the gasoline release to 4,200 gallons. It initially estimated 2,200 gallons. Operators promptly shut

off pressure after diagnosing the problem, but couldn't account for what was still in the line and in the process of seeping out until Friday, said Greg DeBrock, incident commander and Midwest district manager for BP Pipelines North America Inc.
Source: http://c.moreover.com/click/here.pl?j495211217&f=767

9. *March 25, Toledo Blade (OH)* — **Toxic cloud from chemical plant forces dozens to evacuate homes in Ohio.** A chemical reaction inside a holding tank at a hazardous waste facility spewed a cloud of toxic nitrogen dioxide over eastern Sandusky County, OH, Friday, March 24, forcing dozens of residents to evacuate their homes for several hours. Nitrogen dioxide is a red−brown gas that is extremely toxic and can be fatal if inhaled, according to the U.S. Environmental Protection Agency. Contact with the chemical can irritate the eyes, nose, and throat. No serious injuries were reported. The reaction occurred in one of the plant's six 200,000−gallon storage tanks, where liquid waste is held before being injected into the ground at depths of more than 2,000 feet. Officials said it was unclear what was in the tank, which was filled to 92 percent of its capacity when the reaction occurred.
Source: http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20060325/NEWS01/603250440/0/NEWS10

[Return to top]

## Defense Industrial Base Sector

10. *March 27, Aviation Now* — **New review reaffirms CSAR−X strategy; updates due.** A first−of−its−kind, high−level policy review conducted by Department of Defense (DoD) officials last week has reaffirmed the Air Force's proposed combat search and rescue (CSAR−X) aircraft competition, much to industry's relief, as competitors this week will explain how they'd spend an expected infusion to move up the development of Block 10 aircraft. A DoD statement issued Friday, March 24, said the CSAR−X program was "on track" for the planned August review by the Defense Acquisition Board. Industry −− temporarily caught up in the confusing, 11th−hour review −− now expects an August award for the 141−aircraft program.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/CX03276.xml

11. *March 24, Federal Computer Week* — **DoD issues final rule on non−DoD contracts.** The Department of Defense (DoD) has finalized a rule it published on an interim basis in May 2005. The rule establishes that any nonperformance−based contract awarded within DoD or any contract award through a non−DOD contract vehicle must go through a system of approvals.
Source: http://www.fcw.com/article92738−03−24−06−Web

12. *March 24, Air Force Link* — **Air Force releases Unmanned Aerial Vehicle strategic vision.** The Air Force recently completed a vision document to provide high−level guidance to service development and integration of unmanned aircraft for the next 25 years. While the Air Force has been experimenting with Unmanned Aerial Vehicles (UAVs) since 1962, the technology has only recently evolved to a point to provide truly transformational capabilities to the joint commander, said Brig. Gen. Stanley Clarke, deputy director of the Air Force strategic planning

directorate. The Air Force produced the UAV strategic vision document, entitled "The U.S. Air Force Remotely Piloted Aircraft and Unmanned Aerial Vehicle Strategic Vision," primarily in response to recommendations by the 2004 Air Force Futures Game.
UAV vision document: http://www.af.mil/shared/media/document/AFD−060322−009.pdf
Source: http://www.af.mil/news/story.asp?id=123017981

13. *March 24, Federal Times* — **DoD procurement staff faces peer reviews.** About 1,500 Department of Defense acquisition officials will undergo more exhaustive reviews as part of a new effort to ensure procurement integrity. The new “360−degree reviews” will evaluate acquisition officials by considering the views of their peers and subordinates, in addition to the views of their supervisors, said Domenico Cipicchio, acting director of Defense procurement policy, at an industry−sponsored luncheon on Thursday, March 23. The broader reviews are already being done for officials in the office of the undersecretary of Defense for acquisition, technology and logistics.
Source: http://federaltimes.com/index.php?S=1642117

[Return to top]

## Banking and Finance Sector

14. *March 27, ZDNet (Australia)* — **DNS servers do hackers' dirty work.** In a twist on distributed denial−of−service attacks, cybercriminals are using DNS (domain name system) servers −− the phonebooks of the Internet −− to amplify their assaults and disrupt online business. Earlier this year, VeriSign experienced attacks on its systems that were larger than anything it had ever seen before, it said last week. The company discovered that the assaults weren't coming from commandeered "bot" computers, as is common. Instead, its machines were under attack by DNS servers. "DNS is now a major vector for DDOS," Dan Kaminsky, a security researcher said, referring to distributed denial−of−service attacks. "The bar has been lowered. People with fewer resources can now launch potentially crippling attacks," he said. Just as in any DDOS attack, the target system −− which could be a victim's Web server, name server or mail server −− is inundated with a multitude of data coming from multiple systems on the Internet. The goal is to make the target unreachable online by flooding the data connection or by crashing it as it tries to handle the incoming data. DDOS attacks are sometimes used by criminals looking to extort money from online businesses.
Source: http://www.zdnet.com.au/news/security/soa/DNS_servers_do_hackers_dirty_work/0,2000061744,39248309,00.htm

15. *March 27, Wired* — **Cybersquatters try new tactics.** Cybersquatting the domain name of a celebrity and selling it for a king's ransom was one of the great get−rich−quick schemes of the early Internet. But since courts now tend to favor the star over the squatter, a new kinder, gentler cybersquatting tactic has emerged. These days, cybersquatters seek to register a star's domain before that person becomes famous, and then develop a business relationship with the new celebrity, offering Website hosting or design work. These so−called soft squatters are registering the domains of hundreds of amateur athletes, musicians and other would−be stars in the hope that one or two of the names will become well known. In October 2004, spectator Mike Secord registered the names of numerous fledgling, unknown ice skaters, including kimmiemeissner.com. After the Winter Olympics in Turin and a World title, figure skater

Kimmie Meissner is no longer fledgling or unknown.
Source: http://www.wired.com/news/technology/internet/1,70475−0.html

16. *March 24, Channel Register (UK)* — **Trojan intercepts bank tokens.** A newly discovered Trojan is intercepting the TAN codes used as security tokens by customers of two major German banks, Postbank and Deutsche Bank. Until now, TAN codes were pretty safe, in particular against phishing attacks, as these tokens are sent either through (snail) mail or by SMS. Trojan−Spy.Win32.Bancos.pw is changing the security landscape, as it is able to intercept HTTPS traffic and obtain the security token pass code. When the customer tries to enter a TAN code, an error message appears. Phishing scammers, if they are quick enough, can then enter the code themselves.
Source: http://www.channelregister.co.uk/2006/03/24/trojan_captures_token/

17. *March 24, Associated Press* — **Georgia officials say hacker may have accessed retiree files.** Officials said Friday, March 24 that an intruder penetrated three layers of computer security and hacked into a server holding confidential, personal data for more than half a million state retirees. While there is no evidence that the hacker actually accessed the retirees' files, state officials are sending out letters next week urging participants to check their credit reports to ensure they do not become victims of identity theft. The incident occurred between Tuesday, February 21 and Thursday, February 23. The case has been referred to the Georgia Bureau of Investigation. At issue are the files of 188−thousand active members of the retirement system receiving pension benefits. Another 375,000 files are held by the state for people who may have worked for the state for some period of time.
Source: http://www.firstcoastnews.com/news/georgia/news−article.aspx ?storyid=54435

18. *March 24, IDG News Service* — **Russian Website offered eBay account info for $5.** eBay helped to shut down a Russian Website this week that was offering to sell stolen customer account information for as little as $5 each. Armed with an eBay customer's login and password, a scammer could post items for sale, collect payments, and then never deliver the goods. The site was also offering to sell a handful of PayPal accounts. Security vendor Sunbelt Software detected the site Tuesday, March 21, and reported it to eBay, which worked with the local ISP to have it taken offline. The site probably collected the information through phishing attacks or a Trojan horse virus that plants keylogging software on users' PCs, said Alex Eckelberry, president of Sunbelt. The site preferred accounts that were used infrequently, meaning a user would take longer to notice any suspicious activity, and asked a higher price for accounts with good feedback ratings. Prices ranged from $5 to $25 per account.
Source: http://www.infoworld.com/article/06/03/24/76785_HNebayaccountinfo_1.html?source=rss&url=http://www.infoworld.com/article/06/03/24/76785_HNebayaccountinfo_1.html

[Return to top]

## Transportation and Border Security Sector

19. *March 27, Associated Press* — **Airbus evacuation drill causes 33 injuries.** Thirty−three people suffered minor injuries Sunday, March 26, during a crucial evacuation drill for the new

Airbus A380 superjumbo jet held in Hamburg, Germany. One man broke his leg and 32 other people suffered minor injuries during the exercise in which 853 people and 20 crewmembers from airline Lufthansa AG exited the plane on slides in a darkened hangar. Aviation authorities mandate specific evacuation times for jet models, and the drill was a critical test for the jet, which will be the world's largest passenger model when it begins commercial service. Despite the injuries, Airbus said the plane passed its test, with everybody out of the airplane in about 80 seconds. The European Aviation Safety Agency will confirm the test results this week. If the agency decides the test was a failure, the simulation would be repeated next Saturday.
Source: http://www.usatoday.com/travel/flights/2006−03−27−a380−evacu ation−drill_x.htm

**20.** *March 27, Truck News (Canada)* — **Vancouver Port Authority introduces new standards for container trucks.** Starting Monday, March 27, the Vancouver Port Authority (VPA) will introduce new and stronger requirements to its mandatory Truck Licensing System. These will include more rigorous safety, security and environmental standards that will apply to all container trucks and container truck operations at Lower Mainland ports. The new requirements are part of the VPA's response to last summer's withdrawal of services by most Lower Mainland container truckers. Container truck operators will have 60 days to comply with changes designed to improve the flow of container truck traffic on Lower Mainland roadways, reduce wait times at truck gates, reinforce safe driver behavior, and reduce emissions. The VPA's new licensing requirements include mandatory participation in a truck monitoring and vehicle location program, disclosure and sharing of vehicle and driver safety information, enhanced environmental and safety standards, and compliance with designated truck routes.
Source: http://www.trucknews.com/issues/ISArticle.asp?id=54106&issue =03272006&btac=no

**21.** *March 27, Rocky Mountain News (CO)* — **Serial bomber extremely dangerous.** Federal agents in the fourth day of a nationwide manhunt for a serial bomber said on Monday, March 27, the suspect in five bombs in Grand Junction, CO, and another in Tennessee is considered “extremely dangerous” and a potential threat to airports. Robert L. Burke, 54, who had worked as an air traffic controller, is sought on a federal warrant in the Friday, March 24, bombings in Grand Junction, in which two homes of former colleagues had minor damage. No one was injured. “As an air traffic controller, he's obviously familiar with airport operations,” Tom Mangan, an agent with the U.S. Bureau of Alcohol, Tobacco and Firearms, said on Monday. “This is nationwide.” Burke worked 10 years for the Serco Group, a company that provides air traffic controllers to the Federal Aviation Administration in 56 U.S. airports, most of them in the West and Alaska. Burke was fired in 2004. There is 24−hour security at the tower at Walker Field Airport, a step taken as soon as Grand Junction police learned that all five of the targeted homes were occupied by Serco employees.
Source: http://www.rockymountainnews.com/drmn/local/article/0,1299,D RMN_15_4574181,00.html

**22.** *March 26, USA TODAY* — **NTSB investigators sound alarm on Airbus rudder.** Federal aviation investigators say that a plan by jet manufacturer Airbus that urges airlines to inspect certain jets for a possible serious safety problem is "inadequate" and that the inspections need to be done faster. The National Transportation Safety Board (NTSB) has called for a swift round of inspections after damage was found on an Airbus jet that could lead to the type of crash that killed 265 people in New York City. The tail fin, which keeps an aircraft stable, broke off an American Airlines A300 shortly after takeoff in New York on November 12, 2001. The crash

was the second−worst air disaster in this country's history. The NTSB issued an "urgent" recommendation on Friday, March 24, calling for carriers to immediately examine the rudders on A300 and A310 jets. Last fall, FedEx maintenance workers found a three−foot section of the rudder had begun to break apart on one of its A300 jets. Only American Airlines, with 34 A300s, carries passengers on the jet in this country. Three cargo carriers use the A300 or the A310 in the USA, according to the Air Transport Association annual report. The recommendation would apply to about 400 jets worldwide.
Source: http://www.usatoday.com/travel/flights/2006−03−26−airbus−rud der_x.htm

**23.** *March 26, USA TODAY* — **Shortcut included in copter trips to JFK.** A new helicopter service begins whisking passengers from Wall Street to New York's John F. Kennedy International Airport (JFK) on Sunday, March 26 −− and passengers will skip airport security lines. That's because the federal government is sending airport screeners and explosive−detection equipment to the Lower Manhattan heliport so passengers and their bags can be checked before being delivered to the airport. It marks the first time the Transportation Security Administration (TSA) has done screening at a heliport since the agency took over airport security after 9/11. Douglas Hofsass, the TSA official responsible for security at the new heliport, said that if passengers and their bags aren't screened at the heliport, they'd be flying through the city's airspace unchecked. U.S. Helicopter Corp. chief executive Jerry Murphy says the eight−minute rides, which cost $159 each way, will appeal mainly to business travelers who don't want to waste up to two hours in a car or cab fighting New York traffic. Murphy said his helicopters, the first to offer airport service in more than 20 years, also will fly to LaGuardia and Newark airports by the end of 2006. The company expects to carry 150,000 passengers in its first year.
Source: http://www.usatoday.com/travel/news/2006−03−26−heliport_x.ht m

**24.** *March 24, Reuters* — **U.S. airlines hedging more against high fuel costs.** U.S. airlines are hedging more of their fuel costs this year to protect themselves against a possible rise in the price of oil which some expect could eclipse high levels hit last year, according to a Reuters survey of top carriers. After getting smacked by surging fuel costs in recent years as well−hedged rivals such as Southwest Airlines saw their profits rise, many airlines are taking out or expanding fuel futures positions to shield their bottom lines from one of their costliest areas. AMR Corp.'s American Airlines has taken positions to buy 30 percent of first−quarter consumption at $63 a barrel for crude oil and 18 percent of its full−year fuel needs at $60 a barrel, up from between five and eight percent respectively, in 2005. The airline industry has been severely weakened by soaring fuel costs and low−fare competition that makes it difficult for the carriers to raise ticket prices enough to cover costs.
Source: http://www.usatoday.com/travel/flights/2006−03−23−fuel−hedgi ng_x.htm

**25.** *March 24, Department of Transportation* — **New study concludes driver behavior causes most truck crashes.** Drivers of large trucks and other vehicles involved in truck crashes are ten times more likely to be the cause of the crash than other factors, such as weather, road conditions, and vehicle performance according to a new study released by the Federal Motor Carrier Safety Administration (FMCSA). The Large Truck Crash Causation Study was commissioned by FMCSA to review the causes of, and contributing factors to, crashes involving commercial motor vehicles. While previous data focused on specific crashes and/or individual causes of crashes, this study was the first nation−wide examination of all pre−crash

factors. FMCSA will conduct analysis to further examine driver factors such as use of prescription and over−the−counter drugs, speeding, fatigue, inattention, distractions, work environment, and unfamiliarity with the road. The data offer unprecedented detail about the events surrounding truck crashes that are not available anywhere else. The study database eventually will be available to the public to encourage further analysis and increase the knowledge about large truck crash factors.
Study: http://www.fmcsa.dot.gov
Source: http://www.dot.gov/affairs/fmcsa0206.htm

**26.** *March 24, Federal Computer Week* — **Border Patrol to expand UAV usage.** By the end of this month, U.S. Border Patrol officials plan to monitor a larger area of the southwest border with an unmanned aerial vehicle (UAV), which has been in use since September 2005. They plan to add a second one this summer. Chief David Aguilar said on Thursday, March 23, that officials will increase the UAV surveillance footprint from 150 miles to 300 miles in Arizona at the end of this month. And because the program has been a success, officials will start using a second UAV in Arizona by June, he said. The technology has helped agents make more than 1,000 apprehensions and many drug seizures, he said. It's also been valuable in helping improve officers' safety because they can use UAVs in certain situations before they intervene, he said. UAVs also act as a deterrent because agency officials have notified people that some areas are monitored by air, he added. The Border Patrol has been testing UAVs in some capacity since June 2004. Aguilar said the UAV, which can fly 18 to 24 hours consecutively at an altitude of 18,000 feet, has electro−optical/infrared imagers that can view a license plate and distinguish between humans and animals.
Source: http://www.fcw.com/article92733−03−24−06−Web

**27.** *March 23, Department of Transportation* — **Department of Transportation unveils new commuter rail safety system.** The federal government is testing new safety devices for commuter trains that are designed to better protect passengers during crashes, Department of Transportation Secretary Norman Y. Mineta announced on Thursday, March 23. Mineta unveiled the new safety measures and released footage of a crash test of a train equipped with them during a news conference in Glendale, CA, site of a deadly commuter train crash in January 2005. The test, conducted earlier in the day at the Department's rail testing facility in Pueblo, CO, was designed to determine if the safety devices that are part of the Crash−Energy Management system will make the more than 414 million annual commuter train riders safer. Mineta said the crash test of a locomotive and passenger train equipped with special test dummies was the first ever to use the newly designed Crash−Energy Management system. The system includes crush zones that absorb the force of a crash to better protect the parts of trains where passengers sit and operators, spaces. Other devices tested include newly designed couplers, which join two cars together and are built to retract and absorb energy to keep trains upright on the tracks during a crash. New passenger seats and chairs designed with special padding and crushable edges also were tested.
Source: http://www.dot.gov/affairs/dot4106.htm

**28.** *March 22, Department of Transportation* — **St. Lawrence Seaway international section opens.** The St. Lawrence Seaway, the world's longest inland waterway, opened its international section on Thursday, March 23 kicking off what promises to be a busy 2006 navigation season, Seaway Administrator Albert Jacquez announced on Wednesday, March 22. "Steady orders for

outsized project cargo, imports of foreign made wind turbine components, and the possibility of zinc exports suggest this year will be a strong one," said Jacquez. Historically, the Seaway's performance tracks the overall state of the national economy. With construction, manufacturing and farming industries doing well overall, the waterway is likely to reflect that strength with a strong season, he predicted. Jacquez and his Canadian counterpart, Richard Corfe, President and CEO of the St. Lawrence Seaway Management Corporation, also have expressed a desire to attract new cargoes and container shipping into the Seaway.
Source: http://www.dot.gov/affairs/slsdc0106.htm

29. *March 22, Department of Transportation* — **Department of Transportation seeks innovative research proposals from America's small businesses.** Companies are now able to compete for close to $1 million in grant funding from the Department of Transportation for development of research and technology solutions to transportation challenges facing the nation, Department of Transportation Secretary Norman Y. Mineta announced on Wednesday, March 22. Past grant winners have developed, among other things, innovative technologies including safer emergency exit windows for rail passenger cars, devices used by highway maintenance departments to measure pavement strength and resilience, and an automated system to reduce congestion and manage access on America,s highways. The Small Business Innovative Research program provides funding to small businesses to develop commercially viable technologies that will meet federal research and development needs. The goal of the program is to ensure that technologies developing out of this unique program will focus on safer, simpler, and smarter transportation solutions. Research proposals from U.S.−owned businesses of no more than 500 employees are due by May 2, 2006. Grant awards will be made in October.
Solicitation topics and materials: http://www.volpe.dot.gov/sbir/current.html.
Source: http://www.dot.gov/affairs/rita0106.htm

[Return to top]

## Postal and Shipping Sector

30. *March 27, DMNews* — **FedEx wins more flights to China.** FedEx Express, the largest subsidiary of FedEx Corp., said Friday, March 24, that it has the rights to operate three more weekly flights to China, raising its total to 26. These flights were awarded by the U.S. Department of Transportation, effective March 25.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3621 5

[Return to top]

## Agriculture Sector

Nothing to report.
[Return to top]

## Food Sector

31.

*March 24, U.S. Food and Drug Administration* — **Spring water recalled.** North Country Spring Water, Ltd. of Port Kent, NY, is voluntarily recalling all of its bottled water products because the bottled water may be contaminated with total coliform bacteria and diatoms (algae). The New York State Department of Health has confirmed coliform bacteria and diatoms in some samples of bottled water produced by North Country Spring Water, Ltd. Coliform bacteria are naturally present in the environment and are used as an indicator that other, potentially−harmful, bacteria may be present. The presence of coliform bacteria in bottled water is a violation of the New York State Sanitary Code. Coliform bacteria may indicate the presence of other potential contamination. The presence of diatoms can be an indication that untreated or partially treated surface water is contaminating the source water used in the bottling process. North Country Spring Water, Ltd. bottled water products were distributed wholesale in New York, Vermont, and New Jersey where the bottled water was sold to consumers through retail stores and direct delivery.
Source: http://www.fda.gov/oc/po/firmrecalls/northcountry03_06.html

[Return to top]

# Water Sector

**32.** *March 24, South Florida Business Journal* — **Water woes hit development.** South Florida has run out of natural sources of drinking water and will likely experience halted development due to the problem. Major real estate projects in the tri−county area must be curbed until alternative sources of water can be developed, according to the state. Already, it has told Miami−Dade County to reject 17 large−scale projects because of drinking water scarcity. And the creation of alternative water sources will not happen soon. The work will cost of hundreds of millions of dollars and can take decades to complete, according to estimates from regional and local water officials. The Everglades has no more water to give without risking damage to its unique ecosystem, the South Florida Water Management District (SFWMD) warned, and Miami−Dade, Broward and southern Palm Beach counties can no longer solely depend on water from the underground Biscayne aquifer. Further tapping of ground water affects the balance of freshwater pushing back against saltwater intrusion that can spoil wells. Too much use of swamp water threatens restoration of the Everglades, according to the SFWMD.
Source: http://southflorida.bizjournals.com/southflorida/stories/2006/03/27/story1.html?i=33065

**33.** *February 24, U.S. Environmental Protection Agency* — **Point−of−use, point−of−entry treatment devices studied.** Point−of−use (POU) and point−of−entry (POE) water treatment devices are cited in the U.S. Environmental Protection Agency (EPA) Water Security Research and Technical Support Action Plan as a topic requiring further research. POU devices are designed to purify only that portion of incoming water that is being used for drinking and cooking purposes, while POE devices treat all the water coming into a house or facility. The first objective of the study was to conduct a literature review regarding the types of devices and technologies currently available for removing contaminants at the point of use and/or at the point of entry. The most promising technologies and combinations of technologies (e.g., treatment trains) were investigated with regard to their principle of operation; effectiveness for removing radiological, biological, or chemical contaminants; and limitations. The second objective was to examine the potential water security role of POU/POE treatment devices. To

fulfill this objective, different implementation strategies and their ramifications were discussed; issues associated with disposal and residuals management were addressed; and costs, benefits, and limitations from a water security perspective were described. The third objective was to offer a set of recommendations for consideration regarding POU/POE treatment and water security.
Report: http://www.epa.gov/nhsrc/pubs/reportPOUPOE022406.pdf
Source: http://www.epa.gov/nhsrc/news/news022406.htm

[Return to top]

## Public Health Sector

**34.** *March 27, Los Angeles Times* — **Bird flu defies control efforts.** The spread of avian influenza to at least 29 new countries in the last seven weeks is prompting a sobering reassessment of the strategy that has guided efforts to contain the disease. Since February, the virus has cut a wide swath across the globe, felling tens of thousands of birds in Nigeria, Israel, India, Sweden, and elsewhere. Health officials in the U.S. say bird flu is likely to arrive in North America this year, carried by wild birds migrating. The speed of its migration, and the vast area it has infected, has forced scientists to concede there is little that can be done to stop its spread across the globe. The hope was once that culling millions of chickens and ducks would contain or even eradicate the virus. Now, the strategy has shifted toward managing a disease that will probably be everywhere. Officials are hoping to buy a little more time to produce human vaccines and limit the potential economic damage.
Source: http://www.latimes.com/news/science/la−sci−birdflu27mar27,0,1298190.story?coll=la−home−headlines

**35.** *March 27, Associated Press* — **Interpol hosts conference in Singapore on threat of bioterrorism.** Police and officials from several dozen Asian countries gathered Monday, March 27, to discuss bioterrorist attacks, which experts warn could be difficult to immediately detect and could be carried unnoticed by infected victims across continents. Interpol is hosting the three−day workshop on lab security, forensic work, and laws to prevent bioterrorism. Delegates will also assess how to respond to a simulated bioterrorist attack.
Source: http://thestar.com.my/news/story.asp?file=/2006/3/27/apworld/20060327114143&sec=apworld

**36.** *March 27, Agence France−Presse* — **Iraqi man dies of suspected bird flu.** An Iraqi man died from suspected H5N1 bird flu virus in Baghdad, while one member of his family has been admitted for tests on similar suspicions, a spokesperson of the high−level committee to fight bird flu set up by the Iraqi government said. Earlier this year Iraq confirmed deaths of two people from the avian flu in the Kurdistan region of Iraq.
Source: http://news.yahoo.com/s/afp/20060327/hl_afp/healthfluiraq_060327144335;_ylt=AleVqcHUlJwjtqLqGTX3Od6JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

**37.** *March 21, National Institutes of Health* — **Defective immune system response to smallpox vaccine detailed in new study.** Scientists supported by the National Institute of Allergy and

Infectious Diseases (NIAID), part of the National Institutes of Health (NIH), have identified a defect in the immune response of people with the skin condition atopic dermatitis that puts them at risk of developing serious complications following smallpox vaccination. The researchers used laboratory−grown human skin cells to show that an immune system protein called LL−37 is critical in controlling replication of vaccinia virus, the live virus that is the key component in standard smallpox vaccine. The investigators are part of NIAID's Atopic Dermatitis and Vaccinia Network, which was created in 2004 to integrate clinical and animal research aimed at reducing the risk of eczema vaccinatum, a potentially deadly complication of smallpox vaccination. Eczema vaccinatum occurs almost exclusively in people who have a history of atopic dermatitis, a common, non−contagious skin disorder also known as eczema.
Source: http://www.nih.gov/news/pr/mar2006/niaid−21b.htm

[Return to top]

## Government Sector

Nothing to report.
[Return to top]

## Emergency Services Sector

38. *March 27, New York Times* — **New York City conducts a dry run for handling a disaster in the city rail yards.** How would New York City respond if a bomb filled with arsenic trichloride, a highly toxic liquid compound, were to explode on a freight train moving through a Queens rail yard −− just when a commuter train carrying weekend passengers was traveling in the other direction? That nightmarish situation was the basis for a four−hour simulation Saturday, March 26, involving 1,500 police officers, firefighters and other emergency workers and tested the city's ability to respond to a chemical emergency, though not necessarily a terrorist attack. The Office of Emergency Management planned the field exercise, named Trifecta because it emphasized three activities: search and rescue, victim identification and handling of the dead. Despite the grim nature of the exercise the commissioner of emergency management, Joseph F. Bruno, said it demonstrated the effectiveness of the Citywide Incident Management System, a protocol that governs how various city agencies are to interact during a major emergency.
Source: http://www.nytimes.com/2006/03/27/nyregion/27test.html?_r=1&_oref=slogin

39. *March 26, North Jersey* — **As anniversary of TopOff 3 emerges, state and federal agencies fail to issue final drill critiques.** Serious gaps in communication have emerged as one of the problems experienced by hundreds of public agencies and private corporations that participated nearly a year ago in the largest terror drill ever conducted on U.S. soil. Were it an actual emergency, several authorities agree, the results could have been disastrous. "It was a testament to how unprepared people really are," said Wilmer Alvarez, a director at Columbia University's National Center for Disaster Preparedness. "The mistakes that occurred caused almost a complete shutdown of the public health system. They tested the public health system and it got ransacked." As the one−year anniversary of the drill −− known as TopOff 3 −− approaches, neither the state nor federal government has issued final reports detailing the problems −− or

successes −− of the terror simulation. But interviews with government officials and expert observers in recent weeks have drawn parallels to the much−maligned federal response to Hurricane Katrina. In both cases, they said, communication among the dozens of agencies charged with responding to a disaster failed. What's more, leaders on the ground in both the staged drill and the real−world catastrophe possessed a limited understanding of their roles in the National Response Plan.
Source: http://www.bergen.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXkzJmZnYmVsN2Y3dnFlZUVFeXk2OTA1MDcwJnlyaXJ5N2Y3MTdmN3ZxZWVFRXl5Mg==

**40.** *March 24, IDG News Service* — **UK police deploy searchable palm print database.** Police in England and Wales have completed deployment of a searchable palm−print identification system that over the last two weeks has already matched hundreds of prints with potential suspects, according to UK officials. The palm−print system is part of IDENT1, a biometric identity platform that includes 6.5 million sets of fingerprints from the National Automated Fingerprint Identification System.
Source: http://www.infoworld.com/article/06/03/24/76784_HNpalmprintdatabase_1.html?source=rss&url=http://www.infoworld.com/article/06/03/24/76784_HNpalmprintdatabase_1.html

**41.** *March 24, U.S. Department of Defense* — **Report prompts changes in Pentagon's biohazard response.** Pentagon officials released a report Friday, March 24, assessing the Department of Defense's (DoD) reaction to three suspected anthrax incidents in March 2005 and concluding that the department followed correct procedures, but needs to improve notification and coordination. The report by the RAND Corporation, a nonprofit think tank, focuses on mailroom incidents at the Pentagon, the Skyline Towers in Fairfax County, VA, and the Defense Intelligence Agency at Bolling Air Force Base, Washington, DC. The report was a chance for DoD officials to assess their biohazard response procedures and identify areas that needed improvement, said Michael Donley, director of administration and management for the Office of the Secretary of Defense. The most significant area the RAND report identifies as needing improvement is that of the speed and coordination of notification procedures, Donley said. To address this deficiency, the department is drafting a DoD instruction that will include guidelines on notification procedures and incident command, he said. In addition, the Pentagon and the Pentagon Force Protection Agency are sponsoring an exercise, by the name of Gallant Fox, to test threat response, which will take place in May and will include a simulated biological attack on the Pentagon.
Source: http://www.defenselink.mil/news/Mar2006/20060324_4606.html

[Return to top]

## Information Technology and Telecommunications Sector

**42.** *March 27, Secunia* — **Internet Explorer unspecified automatic .HTA application execution.** A vulnerability has been reported in Internet Explorer, which can be exploited to compromise a user's system. Analysis: The vulnerability is caused due to an unspecified error when handling .HTA applications and allows execution of the .HTA application on the user's system without any user interaction when e.g. visiting a malicious Website. Vulnerable

software: Microsoft Internet Explorer 6.x. Solution: Do not visit untrusted Websites. Disabling Active Scripting support may prevent exploitation, but has not been proven.
Source: http://secunia.com/advisories/19378/

**43.** *March 27, IDG News Service* — **Chinese prefer mobile phones over landlines.** Chinese users prefer their mobile phones over landline calling by a growing margin, a trend that is showing up in earnings for Chinese telecommunications companies and government statistics. Convenience, easy access to low cost handsets, the status of talking on a mobile phone and pure necessity for work are all reasons why Chinese users prefer mobile phones, analysts say, and the gap between those with mobiles vs. landlines continues to widen. Government statistics bear this out. China had 393.4 million mobile phone users at of the end of last year, and only 350.4 million landline subscribers, according to China's Ministry of Information Industry. The growth in mobile use comes despite changes at China Telecommunications that might have favored additional landline use.
Source: http://www.networkworld.com/news/2006/032706−chinese−prefer− mobile.html

**44.** *March 26, Websense Security Labs* — **Websense Security Labs: Internet Explorer zero−day update.** To date, Websense Security Labs has discovered more than 200 unique URL's that are using the latest Internet Explorer vulnerability to run exploit code. The most common exploit has been the use of shellcode to run a Trojan Horse downloader.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =451

**45.** *March 24, Security Focus* — **Linux kernel multiple memory leak local denial−of−service vulnerabilities.** Two local denial−of−service vulnerabilities affect the Linux kernel. These issues are due to a design flaw that creates memory leaks. Analysis: Local attackers may exploit these vulnerabilities to consume excessive kernel resources, likely triggering a kernel crash and denying service to legitimate users. For a complete list of vulnerable products: http://www.securityfocus.com/bid/15076/info
Solution: The vendor has released version 2.6.14−rc4 to address these issues.
For solution details: http://www.securityfocus.com/bid/15076/solution
Source: http://www.securityfocus.com/bid/15076/references

**46.** *March 24, IDG News Service* — **Check Point withdraws bid for Sourcefire.** Check Point Software Technologies, an Israeli−owned Internet security company, on Thursday, March 23, withdrew its application to acquire intrusion−prevention firm Sourcefire, whose technology is used to protect the computer assets of the U.S. Department of Defense and the U.S. National Security Agency. This comes amid national security concerns voiced by the Federal Bureau of Investigations and the Department of Defense.
Source: http://www.infoworld.com/article/06/03/24/76772_HNcheckpoint withdraws_1.html

## Internet Alert Dashboard

**DHS/US−CERT Watch Synopsis**

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US−CERT Operations Center Synopsis:** US−CERT is aware of a vulnerability in the way Microsoft Internet Explorer handles the createTextRange() DHTML method. By persuading a user to access a specially crafted webpage, a remote, unauthenticated attacker may be able to execute arbitrary code on that user's system. This vulnerability can also be used to crash Internet Explorer. We are aware of proof of concept code for this vulnerability. More information about the reported vulnerability can be found in the following US−CERT Vulnerability Note:

VU#876678 − Microsoft Internet Explorer createTextRange() vulnerability
http://www.kb.cert.org/vuls/id/876678

Known attack vectors for this vulnerability require Active Scripting to be enabled in Internet Explorer. Disabling Active Scripting will reduce the chances of exploitation. Until an update, patch or more information becomes available, US−CERT recommends disabling Active Scripting as specified in the Securing Your Web Browser document.
http://www.us−cert.gov/reading_room/securing_browser/#how_to_secure

We will continue to update current activity as more information becomes available.

**TSP Phishing Scams**

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. Specifically, sites that provide online benefits are being targeted. Recently, the phishing scam targeted the Thrift Savings Plan (TSP), a retirement savings plan for United States government employees and members of the uniformed services. For more information please see Thrift Savings Plan (TSP) at URL: http://www.tsp.gov/

If you were affected by the TSP phishing scam, please refer to the TSP E−mail scam instructions for assistance. http://www.tsp.gov/curinfo/emailscam.html

US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Additionally, users are encouraged to take the following measures to prevent

phishing attacks from occurring:

Do not follow unsolicited web links received in email messages.

Contact your financial institution immediately if you believe your account and/or financial information has been compromised.

**Current Port Attacks**

| | |
|---|---|
| **Top 10 Target Ports** | 1026 (win−rpc), 6881 (bittorrent), 25 (smtp), 445 (microsoft−ds), 41170 (−−−), 139 (netbios−ssn), 80 (www), 55620 (−−−), 2234 (directplay), 32459 (−−−)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

# Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

# General Sector

Nothing to report.
[Return to top]

**DHS Daily Open Source Infrastructure Report Contact Information**

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

**DHS Daily Open Source Infrastructure Report Contact Information**

| | |
|---|---|
| Content and Suggestions: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644. |
| Subscription and Distribution Information: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information. |

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

## Department of Homeland Security Disclaimer